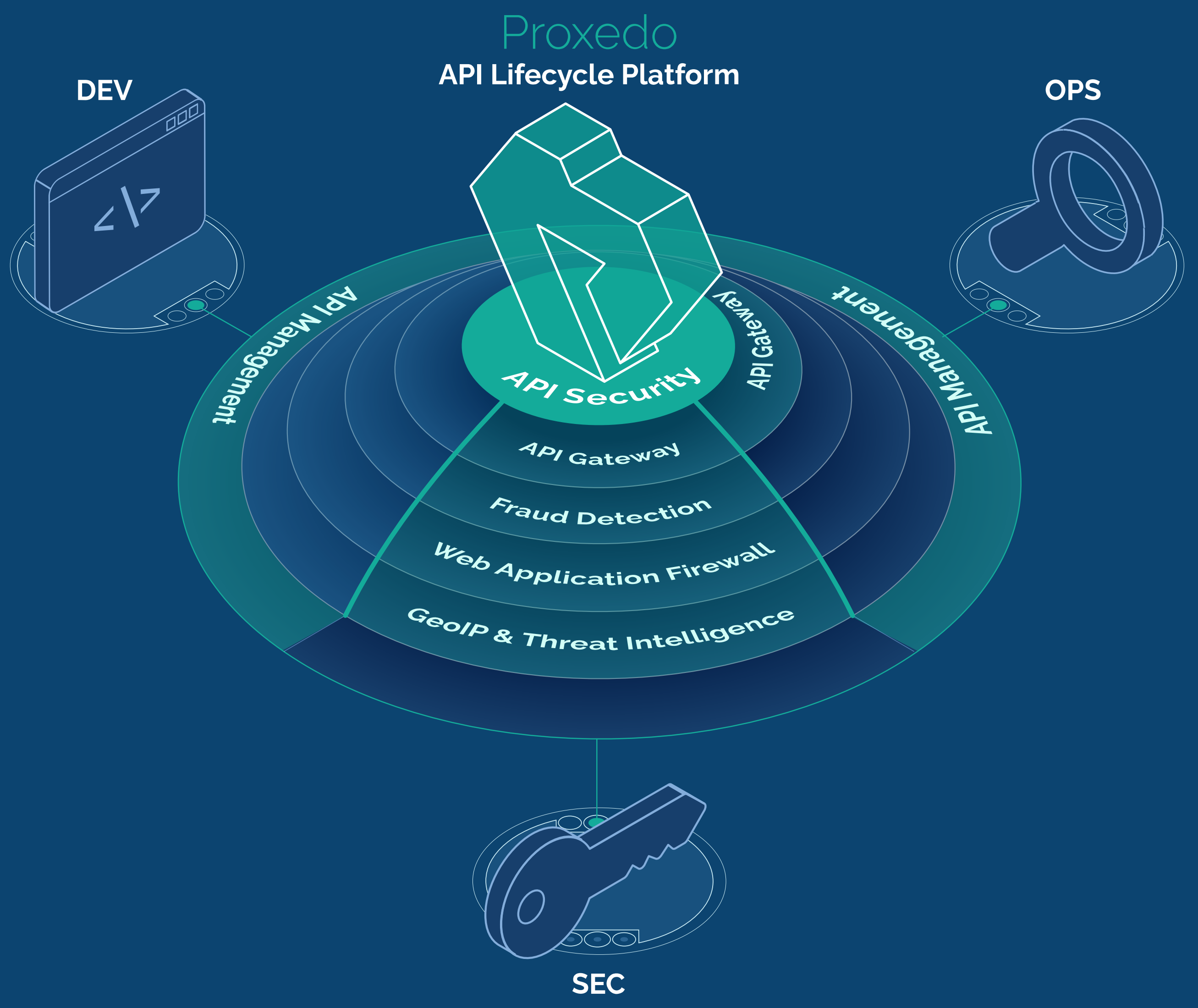

API THREATS ARE OUT OF YOUR TRADITIONAL WAFS REACH

“Gartner predicts that in 2022, application programming interface (API) attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.”

The Challenge

Limitations of WAFs

A web application firewall (WAF) filters, monitors, and blocks HTTP traffic to and from a web application. However, WAFs cannot block targeted API attacks as they are not optimized to fully understand the logic of the API traffic. WAF products are typically optimized for signature-based filtering of HTTP traffic. They are not suitable for in-depth inspection and controlling data flow embedded in API communication. They lack traffic validation, detailed logging, and the ability to implement customized security policies.

So, when it comes to API security, relying solely on your Web Application Firewall gives you a false sense of security. If your company is equipped with an extensive API ecosystem and traditional WAFs, you need a purpose-built API security layer that explicitly addresses the above limitations of WAFs.

BALASYS

info@balasys.eu

The Solution

Proxedo API Lifecycle Platform

The Proxedo API Lifecycle Platform (PALP) is a modular solution that allows you to protect and manage your APIs. PALP provides an end-to-end API security toolset helping your enterprise prevent API-specific threats, automated attacks, APTs and frauds. Its core component is API Security, a specialized security gateway that controls and monitors the API traffic in detail. Beyond the API security core, the portfolio includes API management, web application firewall and fraud detection. PALP provides 360^0 protection of your API environment, adding great value even to your traditional WAF tool.

The following table summarizes the key differentiators of the Proxedo API Lifecycle Platform compared with traditional web application firewalls (WAFs):

Web Application Firewalls	Proxedo API Lifecycle Platform
Focus only on web application protection	Focuses on API security & management, web application protection & fraud detection
Inspection only on HTTP protocol	Inspection on the API layer
Lack of DPI (Deep Packet Inspection)	Advanced DPI
Lack of API call validation	Detailed API call validation
Limited logging capabilities	Customizable traffic & security logging
No flexible policy configuration	Flexible policy configuration & enforcement
Pattern matching based on URL database (blacklisting)	Fully customizable ruleset (blacklisting & whitelisting)

Proxedo API Lifecycle Platform key technical benefits over WAFs

- Understanding and validation of the API traffic content (REST/SOAP)
- API-specific Deep Packet Inspection
- Support of micro-segmentation regarding internal API calls
- Enforcement of customized security policies
- TLS enforcement
- In-depth traffic logging, monitoring, and analytics
- Added security for legacy applications and servers
- API management
- Fraud detection and management

ⓘ

Proxedo API Lifecycle Platform homepage

Request a trial

BALASYS